AN ELEMENTARY SIEVE

DAMIÁN GULICH[A,B]
GUSTAVO FUNES[A,B]
LEOPOLDO GARAVAGLIA[C]
BEATRIZ RUIZ[D]
MARIO GARAVAGLIA[A,B]

[A]Departamento de Física, Facultad de Ciencias Exactas, Universidad Nacional de La Plata, Argentina

[B]Laboratorio de Procesamiento Láser, Centro de investigaciones Ópticas, La Plata, Argentina

[C]Aranjuez, Spain

[D]Centro de investigaciones Ópticas, La Plata, Argentina

E-mail addresses: Damián Gulich: dgulich@ciop.unlp.edu.ar; Gustavo Funes: gfunes@ciop.unlp.edu.ar; Mario Garavaglia: garavagliam@ciop.unlp.edu.ar

Abstract. In this paper we review the properties of families of numbers of the form $6n \pm 1$, with n integer (in which there are all prime numbers greater than 3 and other compound numbers with particular properties) to later use them in a new sieve that allows the separation of numbers n that generate primes from those that only generate compounds. In principle, this can be used to find the amount of prime numbers up to a given number h; this means, $\pi(h)$.

Key words and phrases: Prime numbers, sieve, prime counting function.

1. Introduction

An old problem in mathematics is the way to compute the amount of prime numbers less or equal to a given value h [1, p. 347]. This function is known as $\pi(h)$ [3]. The preeminent method for such task since the 3rd century BC was the sieve of Eratosthenes, and there were no great advances on the subject until the work of Gauss in 1863 [1, p. 352]; which also allowed more advances [2, 5] along with the growth of calculation power in the 20th century. Recent implementations [5] require diverse relatively elaborated computational strategies.

In this paper we will study this problem defining a new sieve whose properties permit an elementary study of $\pi(h)$, and also the possibility of finding its value on a given interval.

2. About the form $6n + 1$

We begin with a very well known result:

Theorem 2.1. *Every prime number of absolute value greater than 3 can be written in the form $6n + 1$ or $6n - 1$.*

Proof. Let's see the equivalences modulo 6. Suppose q prime.

1) If $q \underset{6}{=} 0 \Rightarrow q = 6n \Rightarrow 6 \mid q$, ABS.

2) If $q \underset{6}{=} 1 \Rightarrow q = 6n + 1$, which is not impossible since $7 = 6 + 1$ is a prime.

Date: August 28th, 2007.

n	$\beta_n = 6n-1$	$\alpha_n = 6n+1$
-5	-31 *	-29 *
-4	-25	-23*
-3	-19 *	-17 *
-2	-13 *	-11 *
-1	-7 *	-5 *
0	-1	1
1	5 *	7 *
2	11 *	13 *
3	17 *	19 *
4	23 *	25
5	29 *	31 *

TABLE 1. Values of $6n-1$ and $6n+1$ for several n. With (*) we mark prime numbers.

3) If $q \underset{6}{=} 2 \Rightarrow q = 6n+2 = 2\,(3n+1) \Rightarrow 2 \mid q$, ABS.

4) If $q \underset{6}{=} 3 \Rightarrow q = 6n+3 = 3\,(2n+1) \Rightarrow 3 \mid q$, ABS.

5) If $q \underset{6}{=} 4 \Rightarrow q = 6n+4 = 2\,(3n+2) \Rightarrow 2 \mid q$, ABS.

6) If $q \underset{6}{=} 5 \Rightarrow q = 6n+5 = 6n+6-1 = 6\,(n+1)-1$, which is not impossible since with $n=1$ this gives 11, a prime. □

Definition 2.2. The α class of integer numbers [4] is the set

$$\alpha = \{x \in \mathbb{Z} / x = 6n+1, n \in \mathbb{Z}\} \tag{1}$$

Definition 2.3. The β class of integer numbers [4] is the set

$$\beta = \{x \in \mathbb{Z} / x = 6n-1, n \in \mathbb{Z}\} \tag{2}$$

The different values of relations in (1) and (2) are shown in table 1.

Strictly speaking, a "complete" list of all prime numbers of absolute value greater than 3 ($\{\ldots, -7, -5, 5, 7, \ldots\}$) is the list of primes from both classes.

We now state a property given in [4] where product rules are proved as a theorem:

$\times$	α	β
α	α	β
β	β	α

TABLE 2. Table of products.

Theorem 2.4. *Every prime number of absolute value greater than 3 (except for the sign) is generated by $6n+1$, with n integer.*

Proof. We must prove the equivalence (except for the sign) between both families given in Theorem 2.1.

Let be $f_\alpha(n) = 6n+1$ and $f_\beta(n) = 6n-1$, we mus now prove that $f_\alpha(-n) = -f_\beta(n)$. Indeed:

$$f_\alpha(-n) = 6\,(-n)+1 = -6n+1 = -\,(6n-1) = -f_\beta(n)$$

□

Definition 2.5. We define the set of integer numbers G_α:

$$G_\alpha = \{g \in \mathbb{Z}/6g+1 \text{ is a prime}\} \tag{3}$$

This means, G_α is the set of *all* numbers that (except for the sign) generate *all* primes of absolute value greater than 3 by the relationship (1).

3. The sieve

Definition 3.1. Let A be an infinite matrix whose element $a\,(i,j)$ [1] is

$$a\,(i,j) = i + j\,(6i+1) \tag{4}$$

where $i, j \in \mathbb{Z}$.

Note that numbers on the axis also match this representation.

$$\begin{array}{ccccccccccc}
 & & & & & \vdots & & & & & \\
 & -96 & -71 & -46 & -21 & 4 & 29 & 54 & 79 & 104 & \\
 & -73 & -54 & -35 & -16 & 3 & 22 & 41 & 60 & & \\
 & -50 & -37 & -24 & -11 & 2 & 15 & 28 & & & \\
 & -27 & -20 & -13 & -6 & 1 & 8 & & & & \\
\cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \\
 & 19 & 14 & 9 & 4 & -1 & & & & & \\
 & 42 & 31 & 20 & & -2 & & & & & \\
 & 65 & 48 & & & -3 & & & & & \\
 & 88 & & & & -4 & & & & & \\
 & & & & & \vdots & & & & &
\end{array}$$

3.1. Properties.

Theorem 3.2. *A is symmetrical.*

Proof. A simple expansion shows that

$$a\,(i,j) = i + j\,(6i+1) = i + 6ij + j = j + i\,(6j+1) = a\,(j,i)$$

□

Definition 3.3. Let $\widetilde{A}$ be the set of unrepeated elements of A excluding the axes (the elements of the form $a\,(i,0)$ y $a\,(0,j)$).

3.1.1. *About the signs of the elements of $\tilde{A}$.* Four quadrants can be seen:

$$\begin{array}{ccc}
\text{II} & \uparrow & \text{I} \\
\leftarrow & & \rightarrow \\
\text{IV} & \downarrow & \text{III}
\end{array}$$

What happens to the signs of the elements of $\tilde{A}$ from each quadrant?

Because of Theorem 3.2, we should only focus on the sign of elements of $\tilde{A}$ originally from quadrants I, II, and IV.

- In quadrant I ($i \geq 1$, $j \geq 1$) all elements are positive
- In quadrant II ($i \leq -1$, $j \geq 1$)
  It's easy to see that $j\,(6i+1) \leq 0$, then $\tilde{a}\,(i,j) \leq 0\ \forall i,j$.
- In quadrant IV ($i \leq -1$, $j \leq 1$)
  $i + j\,(6i+1) = i + j + 6ij$. $(i+j) \leq -1$ y $ij \geq |i+j| \geq 1$. Then, the sign is positive.

[1]Coordinates are in the Cartesian sense.

Theorem 3.4. *The elements of $\widetilde{A}$ DO NOT generate prime numbers.*

Proof. $\tilde{a}(i,j) = i + j(6i+1)$ with $i \neq 0$ y $j \neq 0$. If we put this into (1) and suppose p prime, then

$$p = 6\tilde{a}(i,j)+1 = 6(i + j(6i+1))+1 = 6i+6j(6i+1)+1 = (6i+1)+6j(6i+1) = (6i+1)(6j+1)$$

but since i and j are different from zero, then p would be a compound, ABS. □

Remark 3.5. According to the signs of i and j, $6\tilde{a}(i,j)+1$ sweeps (except for the sign) all possibilities:

(1) If $i > 0$ y $j > 0$, the generated number is of the form $\alpha \cdot \alpha$.
(2) If $i < 0$ y $j < 0$, the generated number is of the form $\beta \cdot \beta$.
(3) If i y j have opposite signs, the generated number is of the form $\alpha \cdot \beta$.

See Table 2 for properties of products of α's and β's.

4. Leopoldo's Theorem

Theorem 4.1. *(Leopoldo's Theorem)* $G_\alpha = \mathbb{Z} - \widetilde{A}$

Proof. Every prime number of absolute value greater than 3 is either α or β, and products between those classes of equivalence are closed on themselves. Because of Theorem 3.4 and Remark 3.5, we know that $\widetilde{A}$ generates all possible α and β compound numbers, and so the elements n of $\mathbb{Z} \notin \widetilde{A}$ generate prime numbers by $6n+1$. □

5. Conclusions

Numbers in $\widetilde{A}$ are easy to generate. However, this values are repeated. If an ordering of its elements is possible, then comparing them with $\mathbb{Z}$ will give a list of the values in G_α. The existence of the $\widetilde{A}$-like elements has been known for a long time [1, p. 356], but have been considered impractical to find primes. In this sieve representation, the number of primes between two given values $h_1 = 6c_1 - 1$ and $h_2 = 6c_2 + 1$ where c_1 and c_2 and both are greater than zero, would be

$$\pi(h_2) - \pi(h_1) = 2(c_2 - c_1) - \Lambda(c_1, c_2) + \xi \tag{5}$$

where $\Lambda(c_1, c_2)$ would be a procedure that would count all non repeated values of $\widetilde{A}$ and ξ is a fitting factor. A way of doing this will be the subject of a future paper. Given the value of $\pi(h_1)$, $\pi(h_2)$ would be computable with (5).

6. Acknowledgments

Damián Gulich and Gustavo Funes are financially supported by a student fellowship from the INNOVATEC Foundation, Argentina.

Damián Gulich and Gustavo Funes thank Dr. Mario Garavaglia for involving them in this line of research.

Damián Gulich dedicates this paper to MMB and to his new niece Antonia Monti.

References

[1] Dickson, Leonard Eugene. (1952), *History of the theory of numbers*, (Vol. 1), New York, N. Y.: Chelsea Publishing Company.
[2] Hardy, G. H and Wright, E. M. (1962), *An introduction to the theory of numbers*, (4th ed.), Oxford: Oxford at the Clarendon Press.
[3] Weisstein, Eric W. "Prime Counting Function." From *MathWorld*–A Wolfram Web Resource. `http://mathworld.wolfram.com/PrimeCountingFunction.html`
[4] Garavaglia, Leopoldo and Garavaglia, Mario. (2007), "On the location and classification of all prime numbers". arXiv:0707.1041v1 [math.GM]. `http://arxiv.org`

[5] Deleglise, M. and Rivat, J. (1996), "COMPUTING $\pi(x)$: The Meissel, Lehmer, Lagarias, Miller, Odlyzko method". Mathematics of computation (Vol. 65, N° 213). Jan 1996, P. 235-245.